epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.S. DEPARTMENT OF TRANSPORTATION,

FEDERAL AVIATION ADMINISTRATION

Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned Aircraft Systems

[Docket No. FAA-2015-0150]

April 24, 2015

In 2012, the Electronic Privacy Information Center ("EPIC"), joined by more than one hundred experts and organizations, petitioned the Federal Aviation Administration ("FAA") to undertake a rulemaking to establish privacy regulations prior to the deployment of commercial drones in the national airspace. In the Petition, EPIC described the many ways in which the deployment of drones would threaten important privacy interests.[1] EPIC explained, "[w]ith special capabilities and enhanced equipment, drones are able to conduct far more detailed surveillance, obtaining high resolution picture and video, peering inside high level windows, and through solid barriers, such as fences, trees, and even walls."[2] EPIC also explained that, "[p]ursuant to the FAA Modernization and Reform Act, the FAA is required to: (1) 'develop a

[1] Letter from EPIC, et al., to Michael P. Huerta, Acting Adm'r, Fed. Aviation Admin. (Mar. 8, 2012), *available at* https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf [hereinafter *EPIC 2012 Petition*].
[2] *Id*. at 4.

comprehensive plan' to implement drones into civil commerce; and (2) 'provide guidance on a public entity's responsibility when operating an unmanned aircraft.'"[3] EPIC urged the FAA to "assess the privacy problems associated with the highly intrusive nature of drone aircraft, and the ability of operators to gain access to private areas and to track individuals over large distances."[4] The FAA failed to act on EPIC's Petition. And now, predictably, the problem has gotten worse.[5] As a consequence of the FAA's failure to establish drone privacy rules, millions of Americans now face the possibility of unchecked monitoring and harassment. The Agency must propose new safeguards to address the privacy risks caused by the wide scale deployment of drones.

By notice published on February 23, 2015, the FAA proposed regulations to allow the operation drones in the national airspace system ("NAS").[6] The FAA was required to promulgate these regulations under the FAA Modernization and Reform Act of 2012 ("FMRA")[7] as part of the Agency's "Comprehensive Plan" to safely integrate drones into the NAS.[8] Specifically, the Agency was required to develop a Comprehensive Plan with specific recommendations for a rulemaking to "define the acceptable standards of operation and certification" of drones and to "establish standards and requirements for the operator[s] and

---

[3] *Id*.
[4] *Id*.
[5] *See, e.g*., Kim Lyons, *Privacy Woes at Top of List of Unmanned Aerial Vehicle Concerns*, Pittsburgh Post-Gazette (Apr. 7, 2015), http://www.post-gazette.com/business/legal/2015/04/07/Privacy-woes-at-top-of-list-of-unmanned-aerial-vehicle-concerns/stories/201504070013; Sean Doogan, *Neighbors Worry Over Privacy After Report of Drone Following Kids in Eagle River*, Ala. Dispatch News (Mar. 26, 2015), http://www.adn.com/article/20150326/neighbors-worry-over-privacy-after-report-drone-following-kids-eagle-river; *Drones and Privacy: A Looming Threat*, Economist (Mar. 19, 2015), http://www.economist.com/blogs/democracyinamerica/2015/03/drones-and-privacy; Christina Sterbenz, *Should We Freak Out About Drones Looking In Our Windows*, Bus. Insider (Sep. 24, 2014), http://www.businessinsider.com/privacy-issues-with-commercial-drones-2014-9.
[6] Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9,544 (proposed Feb. 23, 2015) (to be codified at 14 C.F.R. pts. 21, 43, 45, 47, 61, 91, 101, 107, and 183) [hereinafter *Drone NPRM*].
[7] Pub. L.112-95, 126 Stat. 11 (2012) (codified at 49 U.S.C. § 40101 note).
[8] *See id.* § 332, 126 Stat 73–75.

pilot[s]" of drones, as well as identify "the best methods to ensure safe operation" of drones in the NAS.[9] But without adequate privacy rules, drones cannot be safely integrated into the NAS. Privacy rules are a necessary component of the Comprehensive Plan and of the rulemaking required to implement that plan.

By refusing to establish privacy standards or to identify the best methods for mitigating the privacy harms associated with widespread drone deployment, the FAA has failed to satisfy the Congressional mandate issued in the FMRA. The FAA's determination that privacy issues are "beyond the scope of this rulemaking" is not only arbitrary, capricious, and an abuse of the Agency's discretion, it is also contrary to law.[10]

EPIC sued the FAA for denying EPIC's March 8, 2012 petition, and the matter is currently before the U.S. Court of Appeals for the District of Columbia Circuit.[11] EPIC anticipates that, as a result of this suit, the court will overturn the FAA's decision to deny EPIC's 2012 Petition, and require the Agency to conduct a drone privacy rulemaking. But, in addition to the points made in that case, EPIC hereby submits these comments to: (1) underscore the obvious need to establish privacy regulations prior to the deployment of commercial drones in the United States and (2) make clear the specific privacy rules the Agency should have proposed.

EPIC is a non-profit research and educational organization established in 1994 to focus public attention on emerging privacy and civil liberties issues.[12] We work with a distinguished panel of advisors in the fields of law, technology and public policy.[13] EPIC has led the charge for

[9] *Id* § 332(a)(1)(A).
[10] *Drone NPRM*, *supra* at 9,552.
[11] *EPIC v. FAA*, No. 15-1075 (D.C. Cir. filed Mar. 31, 2015).
[12] *About EPIC*, https://epic.org/epic/about.html (2015).
[13] *EPIC Advisory Board*, https://epic.org/epic/advisory_board.html(2015).

strong drone privacy rules.[14] Policymakers and the public alike reference EPIC's reports and webpages as authoritative sources on drone privacy and security.[15]

EPIC has urged Congress to adopt comprehensive legislation to limit drone surveillance. EPIC has informed Congress and state legislatures of the unique threats drones pose, the inadequacy of the current privacy safeguards, and the importance of addressing privacy and civil liberties risks prior to the integration of drones into the NAS.[16] EPIC has been unequivocal in its statements about domestic drones and privacy—use limitations, data retentions limitations, and transparency requirements are essential to preserving privacy and civil liberties as drones are integrated into the NAS.

Earlier this year, EPIC field an amicus brief in the New Mexico Supreme Court calling for the development of clear limitations on aerial surveillance in response to the widespread deployment of drones and the development of increasingly sophisticated but inexpensive surveillance technologies.[17] EPIC has also repeatedly warned the FAA of the privacy and civil liberties risks posed by drones. In addition to the 2012 Petition, EPIC provided extensive

---

[14] EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones* (2015), https://epic.org/privacy/drones/; EPIC, *EPIC v. Army – Surveillance Blimps* (2015), https://epic.org/foia/army/; EPIC, *Spotlight on Surveillance –DRONES: Eyes in the Sky* (2014), https://epic.org/privacy/surveillance/spotlight/1014/drone.html; EPIC, *Spotlight on Surveillance – Unmanned Planes Offer Opportunities for Clandestine Government Tracking* (2005), https://epic.org/privacy/surveillance/spotlight/0805.

[15] *Id*.

[16] *See, e.g.*, *Crimes – Unmanned Aircraft Systems – Unauthorized Surveillance, Hearing on H.D. 620 Before the H. Jud. Comm. of the General Assembly of Maryland* (2015) (statement of Jeramie D. Scott, National Security Counsel, EPIC); *The Future of Drones in America: Law Enforcement and Privacy Considerations Hearing Before the S. Judiciary Comm.*, 113th (2013) (statement of Amie Stepanovich, Director of the Domestic Surveillance Project, EPIC), *available at* https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf.

[17] Brief for EPIC as Amicus Curiae Supporting Respondent, *State v. Davis* (N.M. filed Dec. 8, 2014) (No. 34,548), *available at* https://epic.org/amicus/drones/new-mexico/davis/EPIC-Amicus-Brief.pdf.

comments to the Agency, urging the FAA to establish privacy standards for drone operators at FAA designated drone test sites.[18]

The widespread deployment of drones in the United States is one of the greatest privacy challenges facing the Nation. In the 2012 Petition, EPIC explained that although FAA regulations "only permit civil organizations to operate within the United States with an 'experimental' designation," many individuals have already begun operating drones for commercial purposes.[19] EPIC detailed the many privacy threats posed by widespread drone use. For example, "[g]igapixel cameras used to outfit drones are among the highest definition camera available, and can 'provide real-time video streams at a rate of 10 frames a second.'"[20] EPIC also explained that drones can track "up to 65 different targets across a distance of 65 square miles" and be used to gather sensitive, personal information using infrared cameras, heat sensors, GPS, automated license plate readers, facial recognition devices, and other sensors.[21] The drone use and drones' capacity to facilitate persistent surveillance poses unique threats to privacy; this is especially true because drones, "by virtue of their design, their size, and how high they can fly, [can] operate undetected in urban and rural environments."[22] As EPIC previously explained, these surveillance tools are already being deployed on drones used by paparazzi, private detectives, Google and other mapping companies, and criminals using drones to stalk and harass.

Even the President has recognized that drones pose substantial privacy risks. Earlier this year, the President ordered government agencies to develop new privacy rules and promised that

[18] *Comments of the Electronic Privacy Information Center to the Federal Aviation Administration of the Department of Transportation*, Docket No. FAA-2013-0061 Unmanned Aircraft System Test Site Program (2013), *available at* https://epic.org/privacy/drones/EPIC-Drones-Comments-2013.pdf.
[19] EPIC 2012 Petition, *supra*.
[20] *Id*. at 2.
[21] *Id*. at 2–3.
[22] *Id*. at 3.

"[a]s [drones] are integrated into the NAS, the Federal Government will take steps to ensure that the integration takes into account not only our economic competiveness and public safety, but also the privacy, civil rights, and civil liberties concerns these systems may raise."[23]

The President also stressed that although commercial drone deployment could "enhance American economic competitiveness, our Nation must be mindful of the potential implications for privacy, civil rights, and civil liberties. The Federal Government is committed to promoting the responsible use of this technology in a way that does not diminish rights and freedoms."[24] However, the President did not supplant the FAA's role in carrying out the Comprehensive Plan to integrate drones into the NAS. The President noted that the memorandum "complements and is not intended to supersede existing laws and policies for [drone] operations in the NAS, including . . . the FAA modernization and Reform Act of 2012, the Federal Aviation Administration's (FAA's) Integration of Civil UAS in the NAS Roadmap, and the FAA's UAS Comprehensive Plan."[25]

I. Congress Ordered the FAA to Adopt a Comprehensive Plan to Safely Integrate Drones Into the National Airspace, Including Adopting Rules Necessary to Ensure Safe and Routine Operation

Congress in the FAA Modernization and Reform Act of 2012 (Public Law 112-95) ordered the Transportation Secretary to conduct a public rulemaking to implement "a comprehensive plan to safely accelerate the integration of [drones] into the national airspace system."[26] The plan, in relevant part, must contain "recommendations or projections on"

---

[23] *Memorandum on Protecting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*, 2015 Daily Comp. Pres. Doc. 103 (Feb. 15, 2015).
[24] *Id.* § 2.
[25] *Id.* § 4.
[26] The FAA Modernization and Reform Act of 2012 § 332, Pub. L. 112-95, 126 Stat. 11, 73–75 (2012) (codified at 49 U.S.C. § 40101 note).

> (B) the best methods to enhance the technologies and subsystems necessary to achieve the safe and routine operation of civil unmanned aircraft systems in the national airspace system . . .
>
> (E)–(F) creation of a safe airspace designation for cooperative manned and unmanned flight operations in the national airspace system; . . .
>
> (H) the best methods to ensure the safe operation of civil unmanned aircraft systems and public unmanned aircraft system simultaneously in the national airspace system [.][27]

The Act also requires the Transportation Secretary to determine whether certain drones "may operate safely in the national airspace system."[28] If the Secretary determines that drones may operate safely in the national airspace, the Secretary must "establish requirements for the safe operation of such aircraft systems in the national airspace system."[29]And, as the Agency acknowledges in the NPRM, the FAA Modernization Act's statutory mandate in section 336(b) "preserves the FAA's authority, under 49 U.S.C. §§ 40103(b) and 44701(a)(5), to pursue enforcement 'against persons operating model aircraft who endanger the safety of the national airspace system.'"[30]

II. Drones Cannot Be Safely Integrated Into Or Operated Within The National Airspace Until the FAA Establishes Clear Privacy Rules to Limit Invasive Recording and Prevent Dangerous Self Help

The increasing deployment of drones in the national airspace is one of the most significant threats to privacy faced by Americans today. Drones are flying cameras that "greatly increase the capacity for domestic surveillance."[31] Drones carry increasingly sophisticated recording devices and "by virtue of their design, their size, and how they can fly, can operate

[27] Id. § 332(a)(2)(B), (H).
[28] Id. § 333(a)
[29] Id. § 333(c)
[30] *Drone NPRM*, *supra* at 9,544.
[31] *EPIC 2012 Petition*, *supra* at 2.

undetected in urban and rural environments."[32] These advanced surveillance capabilities greatly surpass those previously available to paparazzi, private detectives, stalkers, and criminals.[33] Drones can even be used to facilitate facial recognition, thermal imaging, or behavioral analysis and tracking. Given the increasingly invasive uses of drones, it is not surprising that individuals are both fearful of and resistant to their deployment.[34] Without adequate privacy rules, drone deployment will be dangerous and continue to create unmanageable conflicts between citizens.

Drones have already been used to take photos of individuals without their consent.[35] Drones enable individuals to harass and stalk unsuspecting victims, taking pictures of them in their homes, places of work, and in public.[36] The type of harassment and stalking that drones facilitate creates a public safety hazard that must be addressed in the Comprehensive Plan. But, the FAA's proposed rule fails entirely to address these varied and significant privacy issues, even though the public has expressed widespread concern and the Agency previously acknowledged that privacy is a necessary component of the Comprehensive Plan.[37]

---

[32] *EPIC 2012 Petition*, *supra* at 3 (quoting Jennifer Lynch, *Are Drones Watching You?*, Electronic Frontier Foundation (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you. *See also* A. Michael Froomkin & Zak Colangelo, *Self-defense Against Robots* 32 (2014), available at http://works.bepress.com/amichael_froomkin/2.

[33] Froomkin & Colangelo, *supra* at 32.

[34] *See* Jason Koebler, *My Neighbor Blasted My Drone With a Shotgun*, Motherboard (Oct. 1, 2014), http://motherboard.vice.com/read/my-neighbor-blasted-my-drone-with-a-shotgun.

[35] *See e.g.*, Joseph, Serna, *As Hobby Drone Use Increases, So Do Concerns About Privacy, Security*, L.A. Times (June 21, 2014), http://www.latimes.com/local/la-me-drone-hobbyist-20140622-story.html (describing incidences of harassment using drones).

[36] *See, e.g.*, *EPIC 2012 Petition*, *supra* at 3.

[37] Scott Neuman, *Commercial Drone Rules To Limit Their Weight, Speed And Altitude*, Nat'l Pub. Radio (Feb. 15, 2015), http://www.npr.org/blogs/thetwo-way/2015/02/15/386464188/commercial-drone-rules-to-limit-their-speed-and-altitude ("Neema Singh Guliani, legislative counsel for the American Civil Liberties Union, says in a statement that the [drone] proposal represents. . . it 'falls short of fully protecting the privacy of Americans.'"); Editorial, *Putting Drones to the Test*, N.Y. Times (Jan. 04, 2014), http://www.nytimes.com/2014/01/05/opinion/sunday/putting-drones-to-the-test.html ("[D]rones can just as easily be used by law-enforcement agencies and big corporations to conduct unconstitutional monitoring of individuals or groups of people. . . . Drones operated by inexperienced or unlicensed pilots pose a hazard to people and property in populated areas.").

A. The FAA Has Already Acknowledged That Rules Governing The Privacy Impact of Drone Operations Should Be Part of the Comprehensive Plan

The FAA has acknowledged, "as the demand for [drones] increases, concerns regarding how [drones] will impact existing aviation grow stronger, especially in terms of safety, privacy, frequency crowding, and airspace congestion."[38]

The FAA's previous adoption of privacy rules for drone test sites made clear that privacy is a necessary component of the Comprehensive Plan. In the FAA's 2013 roadmap report,[39] the Agency acknowledged that the integration will require "privacy considerations."[40] Moreover, the FAA unambiguously stated that Congress required the Agency to address privacy as part of the safe and efficient integrations of drones into the NAS:

> The FAA is responsible for developing plans and policy for the safe and efficient use of the United States' navigable airspace. This responsibility includes coordinating efforts with national security and privacy policies so that the integration of UAS into the NAS is done in a manner that supports and maintains the United States Government's ability to secure the airspace and addresses privacy concerns.[41]

Despite the Agency's clear acknowledgement of the importance of privacy issues in implementing the Comprehensive Plan, the proposed rule fails to address privacy issues as part of the broader drone integration process.

---

[38] Joint Planning and Dev. Office, Fed. Aviation Admin., *Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation's UAS Path Forward* 4 (2013), *available at* https://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf.

[39] Fed. Aviation Admin., *Integration Of Civil Unmanned Aircraft Systems (UAS) In The National Airspace System (NAS) Roadmap* 7 (2013). [hereinafter *FAA 2013 Report*]

[40] *Id.* at 7 ("Integration of UAS into the NAS will require: review of current policies, regulations, environmental impact, privacy considerations, standards, and procedures. . . .").

[41] *Id*. at 11–12.

Moreover, the FAA has previously acknowledged that the Agency is required under the FMRA to develop privacy rules. In 2013, the FAA issued a proposed rule for drone test sites. The FAA stated:

> section 332(c) of [FAA Modernization and Reform Act] directs the FAA, in coordination with the National Aeronautics and Space Administration (NASA) and the Department of Defense (DoD), to develop a [drone] test site program for purposes of gathering safety and technical information relevant to the safe and efficient integration of [drones] into the NAS.[42]

The FAA previously sought public comments on the "proposed approach for addressing the privacy questions raised by the public and Congress with regard to the operation of unmanned systems within the test site program."[43]As a part of the drone test site rules, the FAA found:

> While the expanded use of [drones] presents great opportunities, it also presents significant challenges as [drones] are inherently different from manned aircraft. The [drone] test site program will help the FAA gain a better understanding of operational issues, such as training requirements, operational specifications, and technology considerations, which are primary areas of concern with regard to our chief mission, which is ensuring the safety and efficiency of the entire aviation system. The FAA also acknowledges that the integration of [drones] in domestic airspace raises privacy issues, which the FAA intends to address through engagement and collaboration with the public.[44]

B. The FAA's Failure to Adequately Safeguard Privacy Will Create Safety Risks, Including a Loss of Positive Control Over Drone Operations

The FAA's failure to create drone privacy rules will create the very safety risks the Agency purports to prevent. The FAA has identified two safety concerns in the NPRM. First is the risk of a drone being operated without "the ability to see manned aircraft in the air in time to prevent a mid-air collision between the [drone] and another aircraft."[45] The second is a "loss of positive control" over the operability of a drone "due to a failure of the control link between the

[42] 78 Fed. Reg. 12,259.
[43] *Id*.
[44] *Id*.
[45] *Drone NPRM*, *supra* at 9,548.

aircraft and the operator's control station."[46] The FAA acknowledges that loss of positive control "could pose a significant risk to persons, property, or other aircraft."[47]

Although the FAA acknowledges the significant safety risks posed by a loss of control, surprisingly, the Agency only notes two discrete circumstances in which an operator would experience loss of positive control: (1) when there is a "system failure" or (2) when the operator flies the drone "beyond the signal range or in an area where control link communication between the aircraft and the control station is interrupted."[48] The FAA wholly ignores how industry and individual efforts to prohibit drone surveillance will lead to the loss of positive control and subsequently pose significant risk to persons and property. Efforts to ensure the privacy and safety of individuals on the ground have already led to the development of methods to restrict how drones operate in private air space.

One such technology—known as geo-fencing—involves designating specific areas as restricted air space and programming drones to avoid those areas or be forced to land while in a restricted area.[49] Restricted air spaces may have a large or small geographical footprint such as the entirety of Washington D.C., where flying a drone is prohibited, or a regional airport where drones are prohibited for safety and security reasons. It is not surprising that many individuals

[46] *Id*. at 9,549.
[47] *Id*.
[48] *Id*.
[49] Lily Hay Newman, *Here's How to Set Up a No-Fly Drone Zone Over Your House*, Slate (Feb. 10, 2015), http://www.slate.com/blogs/future_tense/2015/02/10/noflyzone_org_lets_you_geofence_the_area_over_your_house_for_drones_to_avoid.html; *see also* Michael Kushkin, *Drones and cybersecurity Part 2: Solutions*, Federal Times, (February 5, 2015), http://www.federaltimes.com/story/government/it/blog/2015/02/05/drones-and-cybersecurity-part-2-solutions/22936103/(discussing "implementing 'no fly zones' in firmware").

have expressed interest in geo-fencing technologies;[50] individuals do not want drones peering into windows like digital Peeping Toms. To protect their privacy, individuals can add their home addresses to a database of restricted areas made available to drone manufactures for the purpose of programming drones to recognize geo-fenced locations.[51]

However, these self-help techniques will directly impact operators' ability to control their drones—leading to loss of positive control. Therefore, as a result of non-existent privacy regulations, geo-fencing will thwart the FAA's ability to ensure "safe integration" of drones into the NAS.[52] One popular drone manufacture's geo-fencing software removes the operator's control of elevation when flying in a restricted area and forces the drone to immediately land.[53] These types of forced landings pose grave safety risks that the FAA completely disregarded in the current rulemaking.

Rulemaking would allow the public to participate in important issues like whether the FAA should have a say in the composition of any database of geo-fenced air spaces; what safety protocols drone manufacturers should implement for drones that fly into restricted air spaces;

---

[50] Andrew Zaleski, *NoFlyZone, a 'Do Not Call' List for Drones*, Fortune, Feb. 18, 2015, http://fortune.com/2015/02/18/noflyzone-do-not-call-list-drones/ (detailing how over 10,000 people have signed up for the NoFlyZone drone geo-fencing database).

[51] Lily Hay Newman, *supra*; NoFlyZone, https://www.noflyzone.org/ (last visited on Apr. 15, 2015) ("Private property location information will be included in NoFlyZone's comprehensive airspace database provided to participating drone companies. This database includes civil and military airspace, airports, hospitals, schools, and other sensitive locations"); Laura Sydell, Now You Can Sign Up To Keep Drones Away From Your Property, NPR, Feb. 23, 2015 http://www.npr.org/blogs/alltechconsidered/2015/02/23/388503640/now-you-can-sign-up-to-keep-drones-away-from-your-property, ("A new company has set up a way to let drone users know you don't want them over your property. It's called NoFlyZone.org. . .").

[52] 14 CFR § 11.73; *Cf.* Letter from Fed. Aviation Admin. to EPIC (Nov. 26, 2014), *available at* https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf (citing 14 CFR § 11.73 and refusing to conduct rulemaking because the privacy and civil liberties issues were "not an immediate safety concern") [hereinafter *FAA Letter*].

[53] DJI, *No FLY Zones*, http://www.dji.com/fly-safe/category-mc (2015) (explaining in text and video where drones are restricted from entering and how drones react if they successfully enter the restricted areas). *See also* DJI, *Enhanced Safety Features*, YouTube, (Jan. 29, 2015), https://www.youtube.com/watch?v=vimM1nnzljo.

whether it is appropriate for an operator's controls to be in any way disabled while flying in a restricted air space; and other issues that involve the safe operation of drones in a country increasingly interested in taking steps to maintain privacy.

When individuals and drone manufactures are left with no option other than to defend their privacy interests, they will create technologies and react in ways that make operating drones less safe. The privacy, property, and security interests behind the development of geo-fencing are just one example of why it is unreasonable to separate drone privacy from safety, and also why the FAA must conduct rulemaking prior to authorizing widespread drone deployment.

C. The FAA's Failure to Propose Drone Security Rules will Lead to Undue Privacy and Safety Risks

The safe operation of drones depends on the implementation of cyber security measures to prevent drones from being hacked.[54] Drone cyber security not only implicates control and operability of the drones themselves, but also the surveillance equipment installed on drones. Unauthorized access to this equipment could enable widespread privacy invasions and surreptitious monitoring.[55] Drones are equipped with an onboard computer that enables remote control through a communications channel; the same remote control features that make drones easy to operate also make them susceptible to cyberattacks.[56] Hackers can exploit weaknesses in

[54] Evan Carr, National Center for Policy Analysis, *Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace* 20 (2013), *available at* http://www.ncpa.org/pub/unmanned-aerial-vehicles-examining-the-safety-security-privacy-and-regulatory-issues-of-integration-into-us-airspace ("If UASs are easily manipulated by outsiders, the consequences could be grave.").
[55] *Id.* at 26-27, 35.
[56] Michael Kushin, *Drones and cybersecurity part 1: The challenges we face and cybersecurity's role*, Federal Times (Jan. 6, 2015), http://www.federaltimes.com/story/government/it/blog/2014/12/15/drones-and-cybersecurity-part-1-the-challenges-we-face-and-cybersecuritys-role/20450227/

drone software to gain control of a drone's movement and other features.[57] Hackers can also exploit weaknesses in the surveillance devices mounted to drones to access pictures, recorded or live feed video, or other data.[58] There are already publicly available guides that would enable a novice to hack a drone and gain control midflight.[59] These hacks are not complicated or expensive, [60] and drones, like other electronic devices, are exposed to many cybersecurity threats.[61]

The integration of drones into the NAS will mean that thousands of new, hackable devices will be hovering over our homes and streets without any clear security guidance, despite known vulnerabilities. Those vulnerabilities have been recognized since at least 2011, when a university research group demonstrated how to successfully commandeer a hovering drone from a kilometer away.[62] The group used a technique called "spoofing" which involves sending fake GPS signals that trick a drone's receiver as to the drone's location and the time. By spoofing, a hacker can gain full control of a drone's maneuverability. The research group took control of the

---

[57] Pierluigi Paganini, *Hacking Drones . . . Overview of the Main Threat*, Infosec Institute (June 24, 2013), http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/ (explaining how civilian drones use Global Position Systems, or GPS, which can easily be exploited using GPS "spoofing" or jamming devices which trick the drone).

[58] *Id.*

[59] Dan Goodin, *Flying Hacker Contraption Hunts Other Drones, Turns Them Into Zombies*, Arstechnica (Dec. 3, 2015), http://arstechnica.com/security/2013/12/flying-hacker-contraption-hunts-other-drones-turns-them-into-zombies/ (describing the release of specifications to "build an aerial drone that seeks out other drones in the air, hacks them, and turns them into a conscripted army of unmanned vehicles under the attacker's control"); *Which is more dangerous, drone hacking or unsafe drone operation?,* DIY Drones (Dec, 26, 2013) http://diydrones.com/profiles/blogs/which-is-more-dangerous-drone-hacking-or-unsafe-drone-operation (explaining how easy it is to hack into unprotected Wifi linked drone controls).

[60] Pierluigi Paganini, *supra* note 57 (demonstrating that a drone can be hacked with ease and for around $1,000 in equipment).

[61] *Id.* (demonstrating that a drone can be hacked with ease and for around $1,000 in equipment).

[62] Aerospace Engineering and Engineering Mechanics, University of Texas at Austin, *Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV*, http://www.ae.utexas.edu/news/features/todd-humphreys-research-team-demonstrates-first-successful-gps-spoofing-of-uav (last visited Apr. 22, 2015) (describing the drone hacking experiment presented by the university research group at the invitation of the Department of Homeland Security).

drone to illustrate that civil GPS signals are not fully secured and can be "easily manipulated" with grave consequences absent anti-spoofing software.[63]

Experts have warned that the "exploitable weaknesses of the current civilian GPS system present a clear danger for UAS operators and the public living beneath their wings."[64] They have called on the FAA to address these issues in a way that implements "precautionary measures" prior to the full integration of drones into to the NAS.[65] And this is only one example of the insecure nature of current drone control systems.

The FAA must consider the heightened safety issues arising from the hacking of drones and their surveillance equipment.

III. The FAA Should Issue Proposed Drone Privacy Rules

Privacy and safety rules are both necessary and inextricable parts of the Comprehensive Plan to integrate drones into the NAS. Therefore, the FAA's drone NPRM must necessarily include proposed drone privacy rules in order to fulfill Congress's mandate. Because the Agency has failed to include proposed drone privacy rules, the FAA must reissue the current NPRM with proposed privacy regulations. Those proposals should incorporate, at a minimum, the following recommendations:

Use and Data Retention Limitations: Use and data retention limitations should apply to commercial drone operators. Data collected via drone surveillance should not be used for purposes beyond the original reason for collection or beyond the consented use. Similarly, data should not be retained longer than necessary to fulfill the original purpose of collection.

---

[63] Evan Carr, Nat'l Ctr. for Pol'y Analysis, *Unmanned Aerial Vehicles: Examining the Safety, Security, Privacy and Regulatory Issues of Integration into U.S. Airspace* 20 (2013), *available at* http://www.ncpa.org/pub/unmanned-aerial-vehicles-examining-the-safety-security-privacy-and-regulatory-issues-of-integration-into-us-airspace.
[64] *Id.* at 21.
[65] *Id.*

Transparency and Public Accountability: Mechanisms should be implemented to provide ongoing transparency and public accountability in the commercial use of drones for surveillance. These mechanisms should include the following at minimum:

a. *Publicly available collection, use, and retention policies*: Commercial drone operators should post a publicly available document stating its data collection, use, and retention policies.

b. *Publicly available database of commercial drone operators*: A publicly available repository should be created with information on all past and current commercial drone operators in the United States.

c. *Independent Audits*: All commercial drone operators should be subject to independent audits to ensure compliance with their representations.

Minimum Security Standards: The FAA must establish minimum security standards to prevent the loss of positive control and the unauthorized access to the drone's surveillance capabilities or data collected by the drone.

IV. CONCLUSION

For the foregoing reasons, Congress requires the FAA to conduct a public rulemaking to safely integrate drones into the national airspace system. The host of issues involved in the use of drones, which can be used to stalk and spy and have known security flaws, which make them vulnerable to hacking, is an "immediate safety concern."[66] The nature and use of these unique and sophisticated surveillance platforms demonstrate that the potential threats to privacy cannot

[66] *FAA Letter, supra* at 1 ("After reviewing your request, we have determined that the issue you have raised is not an immediate safety concern. Moreover, the FAA has begun a rulemaking addressing civil operation of small unmanned aircraft systems in the national airspace system. We will consider your comments and arguments as part of that project.").

be reasonably separated from the safe operation and integration of drones. Accordingly, the FAA must reissue the current drone NPRM with proposed privacy regulations.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Alan Butler
EPIC Senior Counsel

Khaliah Barnes
EPIC Administrative Law Counsel

Jeramie D. Scott
EPIC National Security Counsel

Jared Galanis
EPIC Law Clerk

Gregory Evans
EPIC Law Clerk

Electronic Privacy Information Center
1718 Connecticut Avenue, Suite 200
Washington, DC 20009
(202) 483-1140